UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/388,002	03/12/2003	Brant L. Candelore	80398P558	6599

8791 7590 05/06/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/388,002	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	SHEWAYE GELAGAY	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23 and 37-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23 and 37-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/23/07,12/7/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on December 7, 2007. Claims 1-23 and 37-49 are pending.

Response to Arguments

2. Applicant's arguments filed December 7, 2007 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 6-8, 12-23, 37-42, 44, 46 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (hereinafter Wasilewski) U.S. Patent 6,157,719 in view of Kocher et al. (hereinafter Kocher) US 6,289,455.

As per claims 1 and 8:

Wasilewski teaches a system in communication with a remote source and a digital device, comprising:

means for receiving a mating key in response to a prior transmission of a mating key generator and a serial number of the digital device to the remote source; (col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26)

means for encrypting a descrambling key with the mating key, the descrambling key being used for scrambling digital content prior to transmission to the digital device; (col. 8, line 39-col. 9 line , line 55; col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26) and

means for transmitting the mating key generator to the digital device. (col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26)

Wasilweski does not explicitly a mating key being a result produced by performing a cryptographic operation on the mating key. Kocher in analogous art, however, teaches a mating key being a result produced by performing a cryptographic operation on the mating key. (col. 9, lines 41-59; col. 11, lines 32-65) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Wasilewski with Kocher in order have improve the security of systems used to distribute and protect digital content thereby minimizing the probability piracy attacks. (col. 5, line 55-col. 6, line 12; Kocher)

As per claims 17 and 21:

Wasilweski teaches an apparatus adapted to receive scrambled content and descramble the scrambled content, comprising: a removable smart card adapted to (i) receive a mating key generator message (col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26) and

(ii) encrypt a descrambling key with a mating key that is generated using the mating key generator message, the mating key generator message includes at least two of a set-top-box manufacturer identifier, a service provider, a conditional access

provider identifier and a sequence number; and; (col. 8, line 39-col. 9 line , line 55; col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26) and a descrambler component to receive the encrypted descrambling key and the mating key generator, the descrambler component decrypts the encrypted descrambling key using the key to recover a descrambling key, the descrambling key being used for descrambling scrambled content loaded into the apparatus. (col. 8, lines 39-67; col. 16, line 19-col. 17, line19; col. 20, lines 42-53; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26)

Wasilweski does not explicitly performing a cryptographic operation on the mating key generator to produce a key that is equivalent to the mating key. Kocher in analogous art, however, teaches performing a cryptographic operation on the mating key generator to produce a key that is equivalent to the mating key. (col. 9, lines 41-59; col. 11, lines 32-65) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Wasilewski with Kocher in order have improve the security of systems used to distribute and protect digital content thereby minimizing the probability piracy attacks. (col. 5, line 55-col. 6, line 12; Kocher)

As per claims 6, 14, 16 and 18:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski further discloses a system comprising: means for generating and providing an entitlement control message (ECM) and an entitlement

management message (EMM) to the digital device alone with the mating key, the EMM comprises at least one key to decrypt the ECM. (col. 9, line 6-col. 10, line 9)

As per claim 7:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilweski further discloses a system comprising: where the descrambling keys are service keys, used to decrypt a channel; and transmitting the encrypted service keys to the digital device. (col. 8, line 39-col. 9 line , line 55; col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26)

As per claims 12-13, 20 and 40:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilwski further discloses a method comprising: transmitting the encrypted data along with the message to a smart card adapted to a set-top box; (col. 8, line 39-col. 9 line , line 55; col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26) and transmitting the encrypted data and the message from the smart card to a descrambler component located within the set-top box. (col. 8, line 39-col. 9 line , line 55; col. 16, line 19-col. 17, line19; col. 22, lines 23-42; Col. 43, line 53-Col. 44, line 26)

As per claims 15 and 23:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski discloses providing meta-data with an electronic program guide in an unscrambled format to the set-top box, the meta-data comprises a plurality of tag entries in which one of the tag entries comprising a channel

name, a name of the digital content, and a key identifier indicating a tier of service associated with the encrypted service key. (col. 7, lines 27-56)

As per claim 19:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski further discloses an apparatus wherein the descrambler component is an integrated circuit. (col. 15, lines 25-43)

As per claim 22:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski discloses wherein the access criteria for accessing a channel is supplied by an ECM in-band with the digital content while the encrypted service key and the corresponding key identifier are contained in an enhancement management message (EMM) supplied out-of-band. (col. 7, lines 27-56)

As per claims 37 and 41:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski discloses wherein prior to receiving the mating key, the method further comprises: performing a cryptographic operation on the message to produce the mating key. (col. 8, lines 39-67; col. 41, lines 50-67; col. 42, lines 1-5; col. 43, line 53-col. 54, line 26 ; col. 6, lines 25-55)

As per claims 38 and 39:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski discloses wherein the performing of the cryptographic operation on the message includes encrypting the message with a key to

produce the mating key. (col. 8, lines 39-67; col. 41, lines 50-67; col. 42, lines 1-5; col. 43, line 53-col. 54, line 26 ; col. 6, lines 25-55)

As per claims 42 and 46:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski discloses wherein the mating key generator includes an identifier of a manufacturer of the set-top box. (col. 22, lines 23-42)

As per claims 44 and 48:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski discloses wherein the mating key generator includes an identifier of a conditional access (CA) provider. Col. 43, line 53-Col. 44, line 26)

2. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (hereinafter Wasilewski) U.S. Patent 6,157,719 in view of Kocher et al. (hereinafter Kocher) US 6,289,455 in view of Giniger et al. (hereinafter Giniger) U.S. Patent Number 6,751,729.

As per claim 2:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. In addition, Wasilewski teaches the manufactures of DHCT maintains a certified database which has the serial number of each DHCT together with the pair of public keys belonging to it and a certificate placed in a database for each of the public keys associated with signatures (col. 22, lines 23-26; col. 47, line 57-col. 48, line 11) Wasilewski teaches a remote source is a mating key server in communication with a

server associated with a manufacturer of the digital device. Both references do not explicitly disclose a plurality of servers each associated with a different manufacturer of digital devices. Giniger in analogous art, however, discloses that a remote source is a mating key server in communication with a server associated with a manufacturer of the digital device. (col. 12, line 60-col. 13, line 2) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Wasilewski and Kocher with Giniger in order to implement a management system that is carried out by different manufacture systems. (col. 12, lines 60-61, Giniger)

3. Claims 3, 9-11, 45 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (hereinafter Wasilewski) U.S. Patent 6,157,719 719 in view of Kocher et al. (hereinafter Kocher) US 6,289,455 in view of Lyle US patent Number 7,242,766.

As per claims 3, 9, 45 and 49:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. Both references do not explicitly disclose a system wherein a mating key sequence number being used to migrate from one mating key to the next. Lyle in analogous art, however, discloses a system wherein a mating key sequence number being used to migrate from one mating key to the next. (col. 11, lines 6-15; col. 27, lines 50-60) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Wasilewski and Kocher with

Lyle in order to use different key to encrypt a protected content. (col. 27, lines 50-60, Lyle)

As per claim 10:

The combination of Wasilewski, Kocher and Lyle teaches all the subject matter as discussed above. In addition, Wasilewski further discloses a system wherein the mating key generator comprises an identifier of a supplier of the digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider. (col. 7, lines 28-56)

As per claim 11:

The combination of Wasilewski, Kocher and Lyle teaches all the subject matter as discussed above. In addition, Wasilewski further discloses a system comprising: means for generating and providing an entitlement control message (ECM) and an entitlement management message (EMM) to the digital device alone with the mating key, the EMM comprises at least one key to decrypt the ECM. (col. 9, line 6-col. 10, line 9)

4. Claims 4-5, 43 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (hereinafter Wasilewski) U.S. Patent 6,157,719 in view of Kocher et al. (hereinafter Kocher) US 6,289,455 in view of Akiyama et al. (hereinafter Akiyama) US patent Number 5,784,464.

As per claims 4-5, 43 and 47:

The combination of Wasilewski and Kocher teaches all the subject matter as discussed above. Both references do not explicitly disclose a system wherein the

mating key generator comprises an identifier of a supplier of the digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider. Akiyama in analogous art, however, discloses wherein the mating key generator comprises an identifier of a supplier of the digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider. (col. 14, lines 35-65) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Wasilewski and Kocher with Akiyma in order to utilize the supplier identification in the key generation process thereby providing further protection for the digital content. (col. 14, lines 35-65, Akiyama)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. G./
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137

Notice of References Cited	Application/Control No. 10/388,002	Applicant(s)/Patent Under Reexamination CANDELORE, BRANT L.	
	Examiner SHEWAYE GELAGAY	Art Unit 2137	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,289,455	09-2001	Kocher et al.	713/194
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.